Mobile Security

Could this scenario happen to you?

You stop at a café to connect to a public hotspot and check your company e-mail. You leave your phone on the table while you grab coffee and a bagel. You sit back down and turn on your phone – it is not locked because you find it annoying to type in a PIN every time you use your phone. You check your bank account before heading back to the office using a local restaurant's Wi-Fi. Using the same open Wi-Fi, you connect to the company server in order to download a client's file… and to download a random puzzle game to play during the boss's lecture!

Most people have probably done at least one of the above, if not more. There are at least **8** instances in this example alone where the phone could have been compromised – meaning your data or device could have been stolen or breached in some capacity.

Fortunately, there are many ways to ensure the security of your mobile device, regardless of whether it is an Android phone, Apple phone, tablet, iPad, laptop or netbook.

Before Purchasing a Device

Precautionary measures are an important and sometimes overlooked step in mobile security. Do extensive research about its security features beforehand. Talk to your cellular service provider about file encryption, VPN access, authentication methods and remote capabilities such as finding and/or wiping your device if it is lost or stolen. Talk to your IT department about an MDM (mobility device management) solution and a Mobility Policy – an often overlooked first step in the process of deploying mobile devices.

Creating and enforcing a mobility policy is very important. Consistency and clear language are key. Be explicit about your expectations. Consider all of your employees when creating your mobility policy. If divvying up a data plan between employees, those who are traveling will use more data than those who are in the office and can use Wi-Fi. Allow for a policy that accommodates each position, yet firm enough to be realistic.

Consider an MDM solution, especially if you are going the Bring-Your-Own-Device (BYOD) route. A mobile device management solution can help protect company devices and enterprise security, as well as providing a variety of other benefits. Consider what MDM solutions your devices will support. It is best to have all devices be uniform throughout the company. That way you do not have to worry about compatibility issues. Many MDMs can accomplish remote wiping, security management and software deployment, easily and efficiently. Device features can be controlled, limiting access to the camera or GPS function. Users could be limited to only downloading certain company-approved applications such as Excel or Chrome.

File encryption and VPN access go hand-in-hand because using a VPN automatically encrypts your data. Think of a VPN as an impenetrable tunnel from your device to the end device. Your data flows through the tunnel and is shielded from hackers. Encryption is when your device garbles your data so that it is unreadable from a hacker's perspective (e.g. "hi" might look like "%$J5"), though the end device/server will be able to decode this and read it. If the device does not have a VPN application or capabilities, one can usually be installed, if the device is compatible.

Remote wipe capabilities are also important. Having an Apple ID on an iPhone will allow the end user to remotely wipe the device. On Android, there are other applications such as Google Device Manager or Samsung Account. As mentioned earlier, an MDM solution can also allow administrators to wipe a device. Additionally, some Exchange servers also have this capability.

Use caution when buying a used phone, especially for employees whose phones contain sensitive company data. Sites like eBay, Craigslist or Amazon can sell phones designed specifically to steal information. When receiving a used device, make sure to check if the IMEI number (in the device Settings) has

Mobile Security

been reported lost or stolen. This can be done through many different websites or by calling the device carrier. Even if it isn't reported as lost or stolen, there may be hidden malicious applications or viruses on the phone. In addition, the device may otherwise be activation locked or have physical defects that aren't obvious such as water damage or cheap replacement parts that are short lived. Because of this, it's best to purchase used phones from trusted sources or direct from manufacturers.

Using Your Device

It is tricky to find a balance between being secure and having quick, easy access to information. More security usually means less convenience, and vice versa. A few questions to ask: Does the device meet the company's mobile security standards? How sensitive is the data being shared? Does it violate the company's mobility policy? If you are unsure of your company's mobility policy, talk to your HR or IT department and ask for a copy of it. And always ask permission before downloading an application (regardless of how safe it is or may seem).

Setting a PIN or Passcode is the simplest way to add an extra layer of security to the device. Employees should always set a PIN or passcode on their work phones. In fact, a lot of companies' mobility policies explicitly state that a PIN or passcode is required to access certain company files or the email server. By setting a reasonably complex PIN or Passcode, it will take hackers months or likely years to break into the device.

Install a mobile anti-virus app – not only can they scan your phone and detect viruses, which is a reactionary measure, they can be used in preventative ways too. They can preemptively warn of suspicious applications, websites and viruses/malware. They can lock a device remotely and make sure to prevent further data breaches (if any were made to begin with). Make sure the anti-virus is from a reputable company. Most of the popular and trusted companies have anti-virus apps (e.g. Norton, Lookout, Kaspersky, etc.). After installation, periodic virus scans should be performed. Some symptoms that may show on an infected device are: exceedingly slow load times, pop ups, added programs not intentionally downloaded, unusual battery drain and/or unauthorized charges on the account.

Use secure encrypted connections when possible. As mentioned earlier, encryption changes data into an indecipherable code. A popular encryption technology is SSL (Secure Sockets Layer). SSL ensures an encrypted connection and should always be checked ON in browser and/or email settings. When inputting sensitive information on a website, such as a credit card number or social security number, it is important that the "HTTPS" is present in the website address. The "S" added on means it is secure. Pay close attention the difference. Some browsers will show a "lock" near the website address when it is securely under HTTPS.

Limit the information stored on devices as much as possible. Employees should never put personal information on a work device or work information on a personal device. There is always a chance that data can be stolen and there is no way of being 100% preventative. However, if the phone is compromised, losing a little sensitive data is better than losing a lot of sensitive data.

Be careful with suspicious media such as applications, websites, e-mails and text messages. Phone applications are notorious for collecting sensitive information to sell to third-party companies. For example, a calculator application should not need to access your contacts or files. In addition, applications from the Apple or Google Play stores can be distributed by anyone. The developer(s) creating the app may have little to no knowledge about mobile security issues, or they may even intentionally distribute a malicious app. Links (within browsers, apps or text messages) should not be clicked if you are unsure how safe it is.

Limit connection to public hotspots and unsecure (open) Wi-Fi networks. A passcode or password is one of the fundamentals of mobile security. A Wi-Fi connection without a password should raise some red flags. Even an amateur hacker can breach an unsecured network within hours and gain access to all devices on that network. If you must connect to an unsecured

network, make sure you are connecting through a VPN and that you have an anti-virus installed.

Disable Wi-Fi, Bluetooth and NFC when not in use. Think of Wi-Fi, Bluetooth and NFC (on Android) as roads. If the roads are open, all kinds of traffic can flow through, including deviant drivers who can cause havoc! While the roads are open, it is good to patrol them to prevent bad behavior. If the roads are closed no traffic can go through, good or bad. This is the same with Wi-Fi/Bluetooth/NFC – if they are ON or "open" there will always be a threat to the device. Some phones are set to automatically connect to any open Wi-Fi. Set Bluetooth to non-discoverable through the Bluetooth settings and turn off NFC under the Android Settings when not in use.

Keep track of the phone – lost and stolen phones are a goldmine for hackers and identity thieves. It may seem like a simple step, but it is easy to forget where you put your phone when you are distracted. If the phone is stolen, quickly report it to the company IT department, then to the local authorities. Remotely wipe the phone if possible. Once the phone has been wiped and reported as stolen, contact the carrier so they can suspend the line or forward the number.

Device End-of-Life

When it's time to say "good-bye" to your devices, it doesn't always have to end on bad terms! Security is still important to the end, so make sure the phone is completely free of information. Not only is this a secure business practice, it can also make sure you get the most value if trading in your phone.

When Trading-in or recycling the device be sure to wipe it properly and securely. If not wiped correctly and completely, someone may be able to still access sensitive information. Check the device's manual or manufacturer website for instructions, and ask the cellular provider for additional help or tips. Make sure any Apple IDs are off the phone before trading it in, otherwise the device will either be sent back or will return no compensation at all.

Do not "root" or "jailbreak" the device. In the past, not many users have done this to their work phones, but with BYOD becoming more popular, unsecured devices are increasingly entering the workplace. "Jailbreaking" and "rooting" are the same concept: removing certain software restrictions set by the Android/iOS operating system, providing the user access to files that are normally prohibited. Most users do this when their device reaches their end-of-life to make them seem newer and better. Not only does this make the device less secure, it may also void the warranty and dramatically reduce (or even completely negate) trade-in value. Many of these users do not realize they are sacrificing security for customization, and developers creating these custom operating systems may not incorporate essential security.